

## ABSTRACT

Provided is a content distribution system that prevents different keys to be derived between an encryption apparatus and a decryption apparatus. A random-number  
5 generating unit 112, in an encryption apparatus 110, generates a random number  $s$ . A first function unit 113 generates a functional value  $G(s)$  of the random number  $s$ , and generates a random-number value  $u$  and a shared key  $K$  from the functional value  $G(s)$ . An encryption unit 114  
10 generates a first cipher text  $c1$  of the random number  $s$ , using a public-key polynomial  $h$  and the random-number value  $u$ . A decryption unit 123, in a decryption apparatus 120, decrypts the first cipher text  $c1$  using a secret-key polynomial  $f$ , to generate a decryption random number  $s'$ .  
15 A second function unit 126 generates a functional value  $G(s')$  of the decryption random number  $s'$ , and generates a random-number value  $u'$  and a shared key  $K'$  from the functional value  $G(s')$ . A comparison unit 127 generates a first re-cipher text  $c1'$ , using the random-number value  
20  $u'$  and the shared key  $K'$ , and outputs the shared key  $K'$  if the first cipher text  $c1$  is equal to the first re-cipher text  $c1'$ .